UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,224	09/12/2003	Partha Bhattacharya	50325-1085	6837

29989 7590 12/08/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
TRAN, MYLINH T	

ART UNIT	PAPER NUMBER
2179	

MAIL DATE	DELIVERY MODE
12/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/661,224	BHATTACHARYA ET AL.	
	Examiner	Art Unit	
	MYLINH TRAN	2179	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,16 and 18-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,16 and 18-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/03/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09/18/08 has been entered.

Applicant's Amendments filed 09/18/08 has been entered and carefully considered. Claims 1-3, 6, 18-20, 23, 25-27 and 30 have been amended. Claim 17 is canceled. However, the limitations of the amended claims have not been found to be patentable over the newly discovered prior art. Therefore, the claims (1-7, 16, 18-31) are rejected under the new ground of rejection as set forth below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-7, 16, 18-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ptacek et al. in view of Houston et al. [US. 2002/0019945].

As to claims 1, 18 and 25, Ptacek et al. teach a method of analyzing security events, comprising: receiving and processing a stream of security events (page 1, 0011), including grouping the security events into network sessions (figure 1), each session having an identified source and destination (figure 3, 318, 322); causing display of a graph on a display of a computer system, the graph representing devices (figure 1) in a network, the devices including security devices (firewall) and non-security devices (disk array), the displayed graph including a plurality of individual device symbols and a plurality of group device symbols (figure 1, 114-1, 114-2, 114-3…), each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network.

Ptacek et al. fail to clearly teach the step of and causing display in conjunction with the graph of security incident information, including causing display, with respect to a group device symbol of a security incident volume indicator that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol. However, Houston et al. teach the security incident

information at 00089 and 0042-0043; a group device symbol of a security incident volume indicator (0044-0046) that indicates a number of network sessions whose source or destination is at the member of a group of non-security devices (0048-0053). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine teachings of Ptacek's network graph with the teachings of Houston. Motivation of the combination would have been to enhance the network analyzing.

As to claims 2, 19 and 26, Ptacek et al. teach upon user selection of a group device symbol for a group of non-security devices, causing display of a second level graph on the display of the computer system, the second level graph representing the non-security devices in the group and the security devices in association with the group (the second level graph is disclosed at figure 2), the displayed second level graph including a plurality of non-security device symbols (figure 2, database of signatures) and a plurality of security device symbols (figure 2, firewall 1-3) , each non-security device symbol representing one non-security device in the group and each security device symbol representing one security device in the group; Ptacek et al. fail to clearly teach the step of and causing display in conjunction with the graph of security incident information, including causing display, with respect to a group device symbol of a security incident volume indicator that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol. However, Houston et al. teach the security incident information at 00089 and 0042-0043;

a group device symbol of a security incident volume indicator (0044-0046) that indicates a number of network sessions whose source or destination is at the member of a group of non-security devices (0048-0053). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine teachings of Ptacek's network graph with the teachings of Houston. Motivation of the combination would have been to enhance the network analyzing.

As to claims 3, 20 and 27, Ptacek et al. teach upon user command with respect to a user specified device symbol in the displayed graph, displaying data representing network sessions whose source or destination is at a device corresponding to the user specified device symbol (page 4, 0060, 0061).

As to claims 4, 21 and 28, Ptacek et al. teach in response to one or more user commands, selecting a network session from the displayed data, and defining a drop rule that comprises a set of network conditions corresponding to the selected network session; wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule (0046-0048).

As to claims 5, 22 and 29, Ptacek et al. teach source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions (0010-0011).

As to claims 6, 23 and 30, Ptacek et al. teach the processing of security events including identifying groups of network sessions that together satisfy a

security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions; wherein each incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol (0046-0068 and 0099).

As to claims 7, 24 and 31, Ptacek et al. teach the processing of security events including excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions (0098-0099).

As to claim 16, Ptacek et al. teach a method of analyzing security events, comprising: receiving and processing security events (page 1, 0011), including grouping the security events into network sessions (figure 1), each session having an identified source and destination (figure 3, 318, 322);

applying a plurality of predefined security event correlation rules to the plurality of network sessions in association with the processed security events (0046-0048); for each of a subset of the predefined security event correlation rules, identifying network sessions from the plurality of network sessions in association with the processed security events, if any, that satisfy the rule (0008-0010);

causing display of a graph on a display of a computer system, the graph representing devices (figure 1) in a network, the devices including security devices (firewall) and non-security devices (disk array), the displayed graph

including a plurality of individual device symbols and a plurality of group device symbols (figure 1, 114-1, 114-2, 114-3…), each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network; Ptacek et al. fail to clearly teach the step of and causing display in conjunction with the graph of security incident information, including causing display, with respect to a group device symbol of a security incident volume indicator that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol. However, Houston et al. teach the security incident information at 00089 and 0042-0043; a group device symbol of a security incident volume indicator (0044-0046) that indicates a number of network sessions whose source or destination is at the member of a group of non-security devices (0048-0053). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine teachings of Ptacek's network graph with the teachings of Houston. Motivation of the combination would have been to enhance the network analyzing.

Response to Arguments

Applicant has argued that Ptacek does not teach or suggest displaying a plurality of group device symbols, each group device symbol representing a group of non-security devices of a network. However, the examiner respectfully disagrees because Ptacek shows plurality of group device symbols (figure 1, SUBNET 1, SUBNET 2, SUBNET 3 and SUBNET 4); each group device

symbol represent a group of non-security devices of a network (figure 1, SUBNET 3 comprising a group of non security devices such as Host 15, Disk Array). Applicant's attention is also directed to page 3, 0031, cited the communications network 1 comprises a series of sub-networks (subnet1-subnet4). These subnets typically include groups of network devices...the subnets include different types of networks devices...

Applicant has also argued that Ptacek does not disclose or teach displaying security incident information in conjunction with displaying a graph of representing devices in network. However, the arguments have been considered but moot in view of the new ground of rejection.

Applicant argued that Ptacek fails to teach incident volume information that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices. However, the arguments have been considered but moot in view of the new ground of rejection.

Further, Ptacek teaches displaying a network security by disclosed at page 3, 0034 plurality of steps of 1) measuring and modeling the services or network communication in legitimate use on the network 1, especially during normal operation of the network, or it lifetime; 2) detecting changes in network usage signatures that suggest attack such as self-propagating network behavior 3) providing access control between different compartments or subnets of the network….

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mylinh Tran. The examiner can normally be reached on Mon - Thu from 7:00AM to 3:00PM at 571-272-4141.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Weilun Lo, can be reached at 571-272-4847.

The fax phone numbers for the organization where this application or proceeding is assigned are as follows:

571-273-8300

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mylinh Tran

Art Unit 2179

/Weilun Lo/

Supervisory Patent Examiner, Art Unit 2179